

Introduction

Welcome to the *Cisco Secure Malware Analytics Appliance Administration Guide*. This chapter provides a brief description of the appliance, the intended audience and how to access relevant product documentation.

- About the Secure Malware Analytics Appliance, on page 1
- What's New In This Release, on page 2
- Audience, on page 2
- About This Guide, on page 2
- User Documentation, on page 3
- Login Names and Passwords (Default), on page 6
- Resetting the Administrator Password, on page 7

About the Secure Malware Analytics Appliance

The Secure Malware Analytics appliance provides safe and highly secure on-premises advanced malware analysis, with deep threat analytics and content. A Secure Malware Analytics Appliance provides the complete malware analysis platform, installed on a Cisco Secure Malware Analytics M5 Appliance server (v2.7.2 and later). It empowers organizations operating under various compliance and Secure Malware Analytics policy restrictions, to submit malware samples to the appliance.



Note

Cisco UCS C220 M4 (TG5400) servers are still supported for Secure Malware Analytics Appliance but the servers are end of life.

Many organizations that handle sensitive data, such as banks and health services, must follow various regulatory rules and guidelines that do not allow certain types of files, such as malware artifacts, to be sent outside of the network for malware analysis. By maintaining a Cisco Secure Malware Analytics Appliance on-premises, organizations are able to send suspicious documents and files to it to be analyzed without leaving the network.

With a Secure Malware Analytics Appliance, security teams can analyze all samples using proprietary and highly secure static and dynamic analysis techniques. The appliance correlates the analysis results with hundreds of millions of previously analyzed malware artifacts, to provide a global view of malware attacks and campaigns, and their distributions. A single sample of observed activity and characteristics can quickly be correlated against millions of other samples to fully understand its behaviors within an historical and global context. This ability helps security teams to effectively defend the organization against threats and attacks from advanced malware.

What's New In This Release

The following changes have been implemented in this guide in Version 2.17:

Table 1: Changes in Version 2.17

Feature or Update	Section
Updated screenshots and instructions.	Configuration Using the Admin UI
New topic for Updates proxy. A SOCKS5 proxy can now be used for downloading updates.	Updates Proxy
New topic for SSH Configuration.	SSH Configuration
Added info on the new Send Test email button	Email
The legacy TGSH-dialog is replaced by a modern Admin TUI	Reconnecting to Admin TUI
The Admin UI now provides a visual cue to allow users to understand whether a RADIUS private key has been installed.	About the Admin UI

Audience

This guide is intended to be used by the Secure Malware Analytics Appliance administrator after the appliance has been set up and configured, and an initial test malware sample has been successfully submitted and analyzed. It describes how to manage organizations and users for the malware analysis tool, appliance updates, backups, and other server administration tasks.

This guide also provides information for administrators who are integrating the Secure Malware Analytics Appliance with other Cisco products and services, such as Cisco Email Security Appliance, Cisco Web Security Appliance, and Secure Endpoint Private Cloud devices.



Note For information about Secure Malware Analytics Appliance setup and configuration, see the *Cisco Threat Grid Appliance Getting Started Guide*.

About This Guide

This guide provides planning information, configuration tasks, and general administrative tasks, and is organized as follows:

Chapter	Description
Introduction	Provides brief description of the appliance, the intended audience, how to access relevant product documentation, log in names and passwords, how to reset the administrator password, and contacting Support.
Planning	Describes the environmental, hardware, and network requirements that should be reviewed prior to setup and configuration.
Network Configuration Using the TGSH Dialog	Provides information about using the Admin TUI to make changes to your initial network configuration, reconnecting to the Admin TUI, and configuring the network in recovery mode.
Configuration Using the Admin UI	Provides information about using the Admin UI to make configuration changes to your appliance. See About the Admin UI for a complete list of tasks that can be performed.
Status	Provides information about viewing system information in the Admin UI, such as installed system packages and their version, detailed logs, and available storage.
Operations	Provides information about activating configuration changes, reloading the Admin UI, managing jobs and power settings, and installing updates.
Support	Provides instructions for starting a live support session and taking support snapshots to aid in resolving issues with the appliance.
Organizations and Users	Provides instructions for creating organizations, managing users, and activating a new device user account.
Inbound and Outbound Connections	Provides information about connecting other Cisco appliances (ESA and WSA), and Secure Endpoint Private Cloud to the Secure Malware Analytics Appliance.
Removing All Data with the Wipe Appliance Boot Option	Describes how to use the Wipe Appliance boot option to remove all data from the Secure Malware Analytics Appliance, including clusters.
CIMC Configuration	Provides information about using the CIMC utility to set up remote server management.

User Documentation

Secure Malware Analytics Appliance User Guides

The latest versions of Cisco Secure Malware Analytics Appliance product documentation can be found on Cisco.com.

C isco.com/c/en/us/support/security/amp-threat-grid-appliance	es/series.html#~tab-documents	* O
Products Support Partners More ¥	cisco	
Support / Product Support / Security /		
Cisco Threat Grid		
Overview Product Overview		
Status Available Order	Product Image Not Available	
Series Release Date 05-JAN-2015		
		Critery Languages
	Contact Cisco 🗸 🗸	Other Languages
Models Documentation Downloads Community	Contact Cisco 🗸 🗸	Other Languages
Models Documentation Downloads Community	Contact Cisco 🗸	Other Languages
Models Documentation Downloads Community Administrator Guide	Contact Cisco 🗸 🗸	Other Languages
Models Documentation Downloads Community Administrator Guide Top Search Results	Contact Cisco 🖌	Other Languages Other Languages X
Models Documentation Downloads Community Administrator Guide Top Search Results Close Terret Grid Appliance Administrator Guide	Contact Cisco V	Other Languages Other Languages X
Models Documentation Downloads Community Administrator Guide Top Search Results Cisco Threat Grid Appliance Administrator Guide v2.5 In Cisco Threat Grid Acolisace Administrator Guide v2.5 In Cisco Threat Grid Acolisace Administrator Guide v2.5 In	Contact Cisco Version 2.5 Includes Windows 10, sample deletion, and Threat Grid portal 3.5.11	Other Languages
Models Documentation Downloads Community Administrator Guide Top Search Results Cisco Threat Grid Appliance Administrator Guide v2.5. Inc. 09 Apr 2020	Contact Cisco Version 2.5 Includes Windows10, sample deletion, and Threat Grid portal 3.5.11	Conter Languages
Models Documentation Downloads Community Administrator Guide <td>Contact Cisco Version 2.5 Includes Windows 10, sample deletion, and Threat Grid portal 3.5.11 Version 2.10 - Administration [Cisco Threat Grid]</td> <td>Conter Languages</td>	Contact Cisco Version 2.5 Includes Windows 10, sample deletion, and Threat Grid portal 3.5.11 Version 2.10 - Administration [Cisco Threat Grid]	Conter Languages

Figure 1: User Guides on Cisco.com

- Cisco Secure Malware Analytics Appliance Release Notes
- Cisco Secure Malware Analytics Appliance Getting Started Guide
- Cisco Secure Malware Analytics Version Lookup Table
- Cisco Secure Malware Analytics M5 Hardware Installation Guide



The Cisco Secure Malware Analytics M5 Appliance is supported in appliance version 2.7.2 and later.

Secure Malware Analytics Portal UI Online Help

Secure Malware Analytics Portal user documentation, including Release Notes, Using Secure Malware Analytics Online Help, API documentation, and other information is available from the ? (**Help**) icon located in the navigation bar in the upper right corner of the Secure Malware Analytics user interface.

L

cisco Threat Grid Submit Sample	Dashboard Samples Reports Indicators Administration V	
D Back to Help Home Page	Welcome to Threat Grid!	
Q. Search X	Cisco Threat Grid is a malware analysis and threat intelligence platform. Threat Grid generates and gathers vast amounts of malware intelligence through	
What's New	static and dynamic runtime sample analysis, as well as from other Cisco integrations. We use that intelligence to maintain libraries of advanced behavioral threat indicators, which we combine with traditional research methods to discover new malware and new behaviors in known malware. Our discoveries are then folded back into our ecosystem, in a continuous process of enrichment of our threat intelligence resources.	
What's New	New to Threat Grid?	
Quick Start	If you're a new Threat Grid user, the quickest way to get up-to-speed is to watch this 15-minute video introduction, which walks you through the interface	
Introduction to Threat Grid Getting Started Submit a Sample for Analysis About the Dashboard	and the primary functions of Threat Grid: • Threat Grid Introduction Quick Start	
Getting Started with Threat Grid APIs Evolution API Dags	Introduction to Threat Grid - Threat Grid Online Help introduction. Gettion Stated - Basic Information about therewere and more	
Doc Search	Advantage server - beact mentioned about networks and mate. About the Deskhoard - Basic information about the dashboard.	
• FAQ	 Sample File Types - Detailed list of sample file types - Detailed list of sample file Types - Detailed list of sample file types. 	
Glossary	Working with Samples - Basic information about viewing samples in Threat Grid.	
Support	 Submit a Sample for Analysis - Step-by-step instructions on how to submit a sample to Threat Grid for analysis. 	
 Threat Grid Videos 	Sample Analysis Report	
About	Search for Samples Doc Search - How to search the online help and API documentation.	
 Behavioral Indicators 	 FAQ - Frequently Asked Questions. If you can't find the answers you need, please let us know! 	
 Entitlements 	Glossary - Threat Grid definitions.	
Feeds	 Support - See Support for instructions on how to request Threat Grid support. 	
Network Exit Network Simulation	Quick Start Videos	
 Playbooks 	Threat Grid Videos	
 Privacy and Sample Visibility 	Threat Grid Demo, July 2018	

Figure 2: Secure Malware Analytics Portal Online Help

Use the online help Search feature located at the top of the left column to find appliance-specific information.

Figure 3: Online Help Search Feature

CISCO Threat Grid Submit Sample	Dashboard Samples Reports Indicators Administration \checkmark	۷ 🛛 🍂 🗸 ۷
*> Back to Help Home Page Q. appliance X What's New	Search results for "appliance" All O Help Only O API Only Hits	
Release Notes What's New	Endpoint / api/v3/configuration/poxe/configs Get/update appliance poke configurations.	
Quick Start Introduction to Threat Grid Getting Stated Submit a Sample for Analysis About the Dashboard Getting Stated with Threat Grid APIs Explore API Docs	Endpoint: /api/v3/doc-tree On an appliance, endpoints not available on the appliance are removed from the result. Endpoint: /api/v3/configuration/cloud-host Retrieves a base URL, name, and description of the current Threat Grid cloud host configured by an applicance administrator.	
FAQ Glossary Support Threat Grid Videos	Help Managing Fireamp Integrations Disposition Update Service Management This topic applies only to Threat Grid appliance users.	
About Behavioral Indicators Entitlements Feeds Network Exit Network Simulation Playbooks Entitlement Semela Michility	Help Managing Organizations However, Threat Grid appliance Organizations are created and managed by appliance administrators, and Organization management tasks are documented in the Threat Grid Appliance Administrators Guide, which is available on the appliance documentation page	1-10 of 19 10 per page

Secure Malware Analytics Portal UI Administration Guide

A portal online help topic is available for administrators, with instructions on how to manage users and other information. Click the **Administration** tab and choose **Administration Guide**.

CISCO Threat Grid Submit Sample	Dashboard Samples Reports Indicators Administration V Q O 🍂 admin V
*> Back to Help Home Page	Administration Guide The following information is primarily intended for Org Admin users.
Q. Search X) What's New • Release Notes • What's New Quick Start • Introduction to Threat Grid • Getting Started • About the Dashboard • Getting Started with Threat Grid APIs • Explore API Docs • Doc Search • FAQ	Managing Organizations Threat Grid Cloud Organizations control Cloud Control are created and configured by the Threat Grid Provisioning team and customer teams as part of the overall process of onboarding new customers. Some Organization management tasks may be performed by org-admin and device-admin users. Threat Grid Appliance Threat Grid Appliances are stand-alone servers that are set up and managed by their owners on-site for enhanced security. The documentation for how to manage organizations on a Threat Grid appliance is located in the Threat Grid Appliance Administrator's Guide, which can be found on the appliance product documentation page on cisco.com . Managing Users You must be logged in as <i>Org Admin</i> (or <i>Admin</i>) to complete the following user management tasks: Creating a New User
Giosary Support Support Threat Grid Videos About Behavioral Indicators Entitlements Feeds Notwork Exit Network Simulation Phytocoks Orden and Sample Misbility	Sending a New User Password URL Updating a User Sending a New User Password Reset URL De-Activating a User Re-Activating a User Re-Activating a User Activating an User Activating an User Activating and User

Figure 4: Administration Guide for the Secure Malware Analytics Portal UI

Email Security Appliance and Web Security Appliance Documentation

For information on connecting an Email Security Appliance (ESA) or Web Security Appliance (WSA), see Integrations.

See the instructions for Enabling and Configuring File Reputation and Analysis Services in the online help or user guide for your ESA/WSA:

- Cisco Secure Email Gateway User Guide
- Cisco Secure Web Appliance User Guide

Login Names and Passwords (Default)

The default login names and passwords are listed in the following table:

User	Login/Password
Admin UI and Shell User	Use the initial Secure Malware Analytics/Admin TUI randomly generated password, and then the new password entered during the first step of the Admin UI configuration workflow.
	If you lose the password, follow the instructions in Resetting the Administrator Password.
Secure Malware Analytics Web portal UI	Login: admin
Administrator	Password: Initialize with the first Admin UI password, and then it becomes independent.

User	Login/Password
CIMC	Login: admin
	Password: password

Password Criteria

Passwords must include the following:

- Minimum of 8 characters
- · At least one number
- At least one special character
- · Uppercase and lowercase characters

Resetting the Administrator Password

The default administrator password is only visible in the Admin TUI during the initial appliance setup and configuration. Once the initial configuration is completed, the password is no longer displayed in visible text.



Note LDAP authentication is available for Admin TUI and Admin UI login when you have multiple administrators. If the appliance is configured for LDAP authentication only, resetting the password in recovery mode will reconfigure the authentication mode to allow login with system password as well.

If you lose the administrator password and are unable to log in to the Admin UI, complete the following steps to reset the password.

Procedure

Step 1 Reboot the Secure Malware Analytics Appliance: click the **Operations** tab and choose **Power**, and then click the **Reboot** button. The appliance reboots, and opens the BIOS window.

Figure 5: BIOS Window - Choose Boot Menu <F6> for Recovery Mode

ıılııılıı cısco

Copyright (c) 2018 Cisco Systems, Inc.

Press <F2> BIOS Setup : <F6> Boot Menu : <F7> Diagnostics Press <F8> CIMC Setup : <F12> Network Boot Bios Version : C220M5.4.0.1h.0.1017180336 Platform ID : C220M5

Processor(s) Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz Total Memory = 512 GB Effective Memory = 512 GB Memory Operating Speed 2666 Mhz M.2 SWRAID configuration is not detected. Switching to AHCI mode.

Cisco IMC IPv4 Address : 100.65.1.219 Cisco IMC MAC Address : A4:53:0E:79:6E:04

Entering Boot Menu ...

92

- **Step 2** In the BIOS window, press **F6** to open the **Boot** menu.
- **Step 3** Choose **Recovery** and press **Enter**.

L

Figure 6: Boot Menu



The Secure Malware Analytics Shell opens in Recovery Mode.

Figure 7: Secure Malware Analytics Shell (tgsh) in Recovery Mode

restarted.
<pre>(29.363085) configure-from-target(1352): net.ipv4.tcp_sack = 1 (0K) Started OpenSSH Deepon</pre>
YOU MUST EXIT TGSH BEFORE METWORK CONFIGURATION CHANGES TAKE EFFECT.
FAILING TO DO SO MAY PREVENT SUPPORT STAFF FROM BEING ABLE TO REACH YOUR SYSTEM.
C 27. 15 Parchet Langet Thread (2010) Backerson Med
No incluse to the TheatCold Shall
Received to the interval of the entre
29.5162181 configure_from-target[13521: net.ind.tcn keenaline_intul = 30
29.566235) configure-from-target[1352]; net. jpd.tcp tw reuse = 1
[29.578452] configure-from-target[1352]: net.core.umen.default = 8388608
[29.590348] configure-from-target[1352]: net.core.rmem.default = 8308608
[29.602073] configure-from-target[1352]: net.core.unem_nax = 8388608
1 29.6134731 configure-from-target[1352]: net.core.rmem_max = 8388608
f 29.6243611 configure_from-target[1352]: net.core.netdev_nax_backlog = 10000
I 29.6350731 configure-from-target[1352]: un.swappiness = 0
[29.645657] configure-from-target[1352]: kernel.shnmax = 77309411328
I 29.6565701 configure-from-target[1352]: kernel.shnall = 10074368
[29.667725] sshd[1433]: Server listening on 0.0.0.0 port ZZ.
[29.680576] sshill(1931) Server Listening on 1: port 22.
(27.032276) sullings): (to threatgrid) root on console
[29.702728] Sul1751: pan_uniX(Su-1)Session): session opened for user threatgrid by (uld=0) (20.702728) sultarially for the line for a formation of the line form and the line formation of the lin
(22,712/200) Systemath): Started Initialize From larget,
1 20.720661 instantili Stating Resold and in a
29.733027 system(11) starten beesten Summer Bole Worker
[29.753293] sustend[1]: Starting DeroSSI Barnon
[29.762993] sustend[1]: Started OwenSSH Daenon.
[29.772456] systemd[1]: Starting Threat681D Recovery Mode.
[29,781763] system([1]: Reached target ThreatGRID Recovery Mode.
[29.791010] systemd[1]: Started ThreatGRID Support Mode Worker.
(29.800165) system(11): Startup finished in 5.581s (kernel) + 23.948s (userspace) = 29.530s.
1 29.8098351 configure-from-target[1352]: Done with importing configuration from target
1 29.8193591 rash-worker[1501]: rash-worker.go:42: BASH worker "FCH1832V319" ready to dial router.
d 30.8275161 rash-worker[1501]: rash-worker.go:55: connected to router "ThreatGBID" at rash.threatgrid.com:19791

Step 4 Run passwd to change the password.

Figure 8: Enter New Password

>> passud [286.653257] sudo[1511]: threatgrid : TTY=tty1 : PWD=/hone/threatgrid : USER=root : COMMAND=/usr/bin/passud threatgrid Enter new UMIX password: [286.663606] sudo[1511]: pan_unix(sudo:session): session opened for user root by (uid=0)

Note

The command prompt is not always visible in this mode and logging output may be displayed at any point on top of your input. This does not affect input; you can keep typing blindly. Ignore the two lines of logging output.

- **Step 5** Enter (blindly) the password and press **Enter**.
- **Step 6** Re-type the password and press **Enter**.

Note

The password will not be displayed.

Step 7 Type **reboot** and press **Enter** to start the appliance in normal mode.

Note

The exit command is no longer required before rebooting for a password reset to take effect (for v2.10 and later).